CIMPA school on Arithmetic, coding and cryptography
National Higher School of Mathematics Sidi Abdellah (Algiers), Algeria, April 5-16, 2026
Problem set on elliptic curve

In this set of exercise we use the following notations: If $E : y^2 = x^3 + Ax + B$, we set

$$\Delta_E = -16(4A^3 + 27B^2) \qquad \text{and} \qquad j_E = -1728\frac{(4A)^3}{\Delta_E} = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Exercise 1. Let $+$ denote the addition law defined in class on the elliptic curve $E : y^2 = x^3 + Ax + B$, and let $O = (0 : 1 : 0)$ be the point at infinity of E,

a) Prove that if P, Q and R are three point E which lie on a line, then $P + Q + R = 0$
b) Prove that $P + Q = Q + P$, for all $P, Q \in E$.
c) Prove that $P + 0 = P$ for all $P \in E$.

Exercise 2. This exercise will be used in the following exercise, if you already know this fact or you are willing to just take it as a fact you can go directly to the next exercise. Given a polynomial f define its discriminant $\Delta(f)$, as

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

where $\alpha_1, \ldots, \alpha_n$, are the roots of f, repeated accordingly to their multiplicity.
Let $f = x^3 + px + q$, prove that $\Delta(f) = -4p^3 - 27q^2$.

Exercise 3. Consider the curve E given by the Weierstrass equation $y^2 = x^3 + Ax + B$, prove that E is non singular if and only if $\Delta_E \neq 0$.

Exercise 4. Prove that two elliptic curve $E_1 : y^2 = x^3 + A_1x + B_1$ and $E_2 : y^2 = x^3 + A_2x + B_2$ are isomorphic over $\overline{K}$ if and only if they have the same j-invariant i.e. if and only if $j_{E_1} = j_{E_2}$.

Exercise 5. The point $(3, 5)$ lies on the elliptic curve $E : y^2 = x^3 - 2$, defined over $\mathbb{Q}$. Find a point in $E(\mathbb{Q})$ different from O with rational, but non integral coordinates.

Exercise 6. The points $P = (2, 9)$, $Q = (3, 10)$, and $R = (?4, ?3)$ lie on the elliptic curve $E : y^2 = x^3 + 73$.

a) Compute $P + Q$ and $(P + Q) + R$
b) Compute $Q + R$ and $P + (Q + R)$. Your answer for $P + (Q + R)$ should agree with the result of part (a)

Exercise 7. Let (a, b) be a point on the elliptic curve E given by $y^2 = x^3 + Ax + B$. Show that if $b = 0$ then $3a^2 + A \neq 0$.